COMPANY NAME	CUSTOMER TYPE	LOCATION
Undisclosed	Manufacturing	Global Operations

Case Study

Building a Scalable OT Cyber Risk Program Across Manufacturing Sites

CHALLENGE

OT security was identified as a critical business risk, with unknown visibility into industrial systems, suppliers, remote access, and site ownership.

SOLUTION

SDG formalized a NIST CSF-aligned OT Cyber Risk Program and delivery model, piloted across an initial eight sites.

RESULT

In six months, SDG provided a scalable foundation with defined goals, objectives, and executive reporting, while pilot sites gained visibility and measurable risk reduction.

SUMMARY

A global manufacturer needed to reduce operational technology (OT) cyber uncertainty across production sites through measurable change, not another point-in-time assessment. Leadership required an operating model that could make site-level OT risk visible to the enterprise without disrupting production.

SDG helped establish a repeatable OT Cybersecurity Maturity Program covering governance, local-site delivery, templates, and executive reporting, while rolling it out across a pilot group of eight locations. Local-site efforts also used Horizon H3 to validate OT network segmentation and identify critical security gaps.

The result was a NIST CSF-aligned program with agreed-upon metrics, stronger site awareness, and executive-ready reporting scalable to future sites.

IN DEPTH: CHALLENGES

The client needed to translate inconsistent site-level OT conditions into an enterprise risk view that leadership could use to prioritize remediation, assign accountability, and scale governance across varied manufacturing environments. Specific challenges to overcome:

- **Enterprise Visibility:** Leadership lacked a consistent view of cybersecurity risk across OT/ICS environments.
- **Site Coordination:** Operations, Facilities, Manufacturing, Engineering, IT, and Cyber needed a shared process without slowing production.
- **Inventory Gaps:** Reliable records of OT assets, shared accounts, and system owners were incomplete or inconsistent across sites.
- **Supplier and Remote Access Risk:** Supplier dependencies and remote access tools were not consistently tracked.
- **Ownership Clarity:** Systems, suppliers, and action items needed named owners.
- **OT Network Testing:** Most local site networks, especially OT environments, had not been tested to validate segmentation or identify critical exposure paths.
- **Maturity Measurement:** Leadership needed a NIST-aligned maturity view to compare sites and plan future readiness cycles.

SOLUTION

SDG established a repeatable OT Cybersecurity Maturity Program and piloted it across the first eight sites. The program gave the client a practical way to coordinate local teams, capture inventory data, track evidence, assign owners, and report progress.

- **Operating Model:** Built a standardized playbook for managing OT readiness consistently across locations.
- **Site Process:** Replaced ad hoc site work with a predictable path from kickoff through reporting.
- **Local Task Forces:** Helped form local cyber task forces across site and enterprise stakeholders.
- **Inventory Workstreams:** Mapped systems, accounts, suppliers, remote access paths, evidence, and findings.
- **Training and Awareness:** Supported training and awareness activities as needed.
- **OT Network Testing:** Used Horizon H3 to support OT network testing and validation activities.
- **Evidence Tracking:** Centralized site evidence into a consistent working structure.
- **Action Tracking:** Owner-assigned remediation actions with clear follow-up.
- **Executive Reporting:** Turned site-level updates into leadership views of progress, open items, and next steps.

RESULTS

The pilot turned an undefined OT readiness effort into a working program the client could measure, manage, and scale. Across the first eight sites, SDG established the structure required to move from local uncertainty to ongoing improvement. Key outcomes included:

- **Baseline Visibility:** Supported development of initial inventories across OT systems, accounts, suppliers, remote access paths, and supporting evidence.
- **Measurable Maturity:** Established initial maturity scores across key domains, creating a consistent framework to benchmark maturity across all sites.
- **Remediation Governance:** Created a structured process to track gaps, owners, actions, evidence, and maturity movement over time.
- **Executive Reporting:** Provided leadership a consistent view of site progress, common gaps, open actions, and next-step priorities.
- **Scale Path Defined:** Validated the model across eight sites and developed a path to expand across the next 16.

CONCLUSION

SDG helped the client establish the operating foundation for maturing OT Security. Across the first eight sites, fragmented local information was normalized for baseline visibility, reduced exposure, clearer ownership, and trackable follow-up. This enabled a scalable OT Cybersecurity Maturity Program that connects site-level execution to enterprise governance, executive reporting, and repeatable remediation cycles.

ABOUT SDG

With more than 30 years of experience partnering with global brands on complex business and IT challenges, SDG is a proven leader in advisory, transformation, and managed services that enable leaders to confidently execute AI, identity, threat, and risk management solutions that protect assets and provide business value. Learn more at www.sdgc.com.

Contact Us: solutions@sdgc.com

SDG

75 North Water Street
Norwalk, CT 06854
203.866.8886
sdgc.com